FERC Order 706
Overview
Disclaimer

This NPCC TFIST workshop provides a forum for the presentation and discussion of member experience in the implementation of compliance programs for the NERC CIP Cyber Security Standards. Materials presented or discussed are the presenters’ own interpretation and recommendations and do not necessarily represent those of their organizations or NPCC.
FERC Order 706

Synopsis:

- Date issued January 18, 2008
- Date effective, 30 days from date appearing in the Federal Register
- Cyber Security Standards Accepted
- Directives issued
- NERC’s Implementation Plan Accepted
Standards and Accepted Items

- CIP-002-1, Critical Cyber Asset Identification
- CIP-003-1, Security Management Controls
- CIP-004-1, Personnel & Training
- CIP-005-1, Electronic Security Perimeter(s)
- CIP-006-1, Physical Security of Critical Cyber Assets
Standards and Accepted Items (more)

- **CIP-007-1, Systems Security Management**
- **CIP-008-1, Incident Reporting and Response Planning**
- **CIP-009-1, Recovery Plans for Critical Cyber Assets**
- **Implementation Plan**
Until FERC approves NERC’s updates the existing Standards remain in effect

- 3 major directives
- Specific Requirements
- Two annual surveys until AC phase
- Not part of Readiness until later
FERC Order 706
3 Major Directives

- Remove “reasonable business judgment”

- Remove “acceptance of risk”

- Develop specific conditions that must be satisfied to invoke “technical feasibility” exception
Technical Feasibility

Exceptions

- Should allow for operational considerations
- Dealt with on a case-by-case basis, but needs framework for sound decisions
  - Develop / implement interim mitigation steps
  - Develop / implement plan to eliminate the exception
  - Report and justify each exception
Questions or Comments?